

REMARKS

Claims 1-8, 10-25, 27-28, 31-45, 47-61, 63-68, 70-75, 77-87, 89-105, 108-128, 131-145, and 149 are pending in this application. All of the pending claims are rejected. Claims 1, 16, 28, 40, 61, 68, 75, 87, 99 and 122 are currently amended. Support for the amended claim language is in the specification at page 11, lines 1-12. Claims 145 and 149 are cancelled. Reconsideration and further examination are respectfully requested.

The presently claimed invention concerns a technique by which the authentication of a host device by a key server can be verified by a designated device. In particular, after authenticating the host device, the key server provides the host device with an access token that can be presented to the designated device to prove that the host has been properly authenticated by the key server. The access token includes a host identifier which identifies the host, a token identifier which identifies the token, and a group identifier which identifies the multicast group for which the host has been authenticated. Further, the token identifier is used by the designated device to obtain a group identifier and authentication key from memory in order to verify authentication of the host device.

All of the pending independent claims are rejected under 35 U.S.C. 103(a) as being unpatentable over US 5,748,736 (Mitra) in view of US 6,088,451 (He). The Examiner cites Mitra at column 7, line 52 through column 8, line 10 for details regarding the initial authentication procedure. Because the cited passages are lacking in detail, the Examiner makes several assumptions about the access information provided by the GSC (being compared with the claimed key server). With respect, the focus would be more fairly directed to Mitra at column 11, lines 8 through 63 where three different techniques for authentication verification are actually

described. In particular, Mittra suggests either (1) the GSC (key server) sends a message to the receivers (designated devices) with the identification of the sender (host device); or (2) the GSC (key server) provides the sender (host device) with a digitally signed certificate having a timestamp and the sender's (host device) identification; or (3) the GSC (key server) digitally signs each message when it is multicast. Surely the Examiner will agree that techniques (1) and (3) are irrelevant to the recited claims, and that technique (2) differs in that there is no token identifier which can be used by the receiver (designated device) to obtain a group identifier and authentication key from memory in order to verify authentication of the sender (host device), as recited in each of the independent claims.

The Examiner cites He at Figure 2 and column 30, lines 8-27 as describing an access token and token identifier. Applicant respectfully traverses. Note how He describes use of the SecureID token: "the authentication server can generate a unique challenge to the user ... the effectiveness of token authentication rests on whether the challenges and responses can be made unpredictable and less likely to be repeated within a short period of time." This is distinct from the claimed access token in two ways. (1) He is describing initial authentication rather than verification of an authentication already performed by another device. (2) The presently claimed access token is not used in a challenge-response test. Further, note that He fails to describe using a token identifier to obtain a group identifier and authentication key from memory in order to verify authentication of the sender, as recited in each of the independent claims.

The dependent claims further define the invention. If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Withdrawal of the rejections of claims 1-8, 10-25, 27-28, 31-45, 47-61, 63-68, 70-75, 77-87, 89-105, 108-128, 131-144 is therefore requested.

Conclusion

For the reasons stated above, the pending claims are allowable over the cited references. Should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Holmes W. Anderson, Applicants' Attorney at 978-264-4001 so that such issues may be resolved as expeditiously as possible.

12/27/2007
Date

Respectfully Submitted,

/Holmes W. Anderson/
Holmes W. Anderson, Reg. No. 37,272
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-4001

Docket No. 120-147